Getting Started with IEC 80001:

Essential Information for Healthcare Providers Managing Medical IT-Networks

AAMI

Getting Started with IEC 80001

Essential Information for Healthcare Providers Managing Medical IT-Networks

Todd Cooper, Yadin David, & Sherman Eagles

AAMI
Association for the Advancement
of Medical Instrumentation

This publication is intended to be a helpful information resource. It is not to be construed as an interpretation of AAMI standards, nor does it constitute legal or regulatory advice. AAMI does not issue interpretations of standards except under very limited circumstances under a formal organizational policy that includes specific procedures as a part of AAMI's consensus process for standards.

All AAMI standards, recommended practices, technical information reports, and other types of technical documents developed by AAMI are voluntary, and their application is solely within the discretion and professional judgment of the user of the document. Occasionally, voluntary technical documents are adopted by government regulatory agencies or procurement authorities, in which case the adopting agency is responsible for enforcement of its rules and regulations.

The views expressed in this publication do not represent the views of AAMI or any AAMI Standards Committee or U.S. Technical Advisory Group administered by AAMI. Standards and information concerning the content of standards that the external authors may include within these materials are subject to change as a result of ballot and public review.

Published by the
Association for the Advancement of Medical Instrumentation
4301 N. Fairfax Drive, Suite 301
Arlington, Virginia 22203-1633

Printed in the United States of America

ISBN 1-57020-408-X

TABLE OF CONTENTS

Page

LIST OF TABLES

LIST OF FIGURES

FOREWORD

REGULATORY PERSPECTIVE

With the best will in the world, medical device regulators cannot do it alone. Lawmakers provide us with tools to protect and promote the public health, but it is the nature of a democracy for the regulators to be one step behind the marketplace they regulate. It's an imperfect setup, but I know I would rather live in a democracy where the regulators have to keep playing catch-up than in some other 'ocracy where the regulators are ahead of the marketplace.

So what else can regulators bring into their mission to get their job done? Standards, science, and humility. That's about all regulators need to complement their laws and regulations!

After we, in the U.S Food and Drug Administration (FDA), had received a disturbing cluster of reports about cyber attacks on hospitals in 2003 and 2004, we set our minds on creating a cybersecurity guidance document for manufacturers and users of medical devices, which would ensure that marketed devices would integrate seamlessly into the medical IT-networks which are their point of use.

Well, that was the theory. The lawyers soon told us we could not aim a guidance document at the user community because we didn't regulate this community.

It was as easy as that.

But it was clear that by leaning only with our regulatory authority on the manufacturers, we would not be achieving much in the very place where the devices are most at risk, their point of use. It was a classic case in which the ability of regulators to effect a meaningful change in the marketplace was constrained by the scope of the law.

So after we published our cybersecurity guidance, now directed at the manufacturers, we went back to school on the whole concept of network integration of medical devices.

Going back to school for a regulator often means getting out of the office and talking to the constituency, so I determined to attend as many biomed, security, and IT conferences as I could during 2005. It was a real eye opener.

What was needed was a change in people and their organizations, not in the law. In the point of use of most computer-controlled medical devices, the IT department often was run by different folks than the biomedical department, each reporting through different channels. The very nature of the networking in which both these groups participated differed markedly.

These two groups were not even on parallel technical tracks. They were on orthogonal vectors, spinning away from each other. No amount of FDA regulation could fix that. But I have always observed that a well-crafted standard can make real changes in the way a profession works. I asked myself, "What if there was a standard for integrating devices into IT-networks that used the bidirectional conveyance of risk management information to provide the basis for proper integration?" This would force the two communities to act together.

So in my non-regulator guise I asked a group of device manufacturers, network specialists, and biomedical professionals to come to Washington in December of that year. There, I asked them the same question. I think a lot of folks around that cold table in an unheated FDA conference room thought, "Is he crazy or was that a good idea that I should have thought of?"

And so it began. Todd Cooper and Sherman Eagles marshaled the standards community while Nick Mankovich marshaled the manufacturers. Many others brought their communities along too. I just went along with the flow since they had all the energy—and the less you do as a regulator in these circumstances the better, I thought.

As the months went by and became years we saw, together, the small-scale feuding between parties subsiding and the will emerging that this could indeed create the basis for next-generation hospital IT administration, where a unified network architecture is protected by the common semantic framework of standard compliance and the partnership of the previous antagonists.

Ah! Good times.

So what's in it for regulators? Well, to start with, we get the power of international standards, and therefore the marketplace, to move us in the direction we want to move but where we have no authority to be. Remember our mission is to "protect" and "promote." Too rarely do we get to promote. This was my chance!

Additionally, we get the industry to define the broad outline of what it wants to share with customers with regard to design criteria available for mitigation of cybersecurity threats in their devices.

No private-sector manufacturer wants to share its intellectual property with its customers, but the feature set of what can be configured might be an attractive marketing tool. This is, in fact, what we regulators would like to see during premarket assessments. So rather than the regulators demanding to see everything and asking about things that might not be relevant, we get the manufacturers to tell us everything relevant right away! This can be formalized as part of the labeling and can be seen by the public and future generations of information system security officers (ISSOs) when internationally standardized Structured Product Labeling initiatives begin in the future.[1]

Additionally, while cybersecurity aspects are prominent, they are not the only aspects that can be injected into the risk communication stream between vendor and purchaser. Consider, for example, wireless technologies and their need for coexistence. There will surely be more.

By now you see the real reason why we regulators want to see IEC 80001 succeed. The days of a nice, closed medical device that can be perfectly assessed for its risks by a stodgy regulator and then allowed onto the market are almost gone forever. Given that about 50% of medical devices that come onto the market now have software in them, the design and the manufacture of medical devices now continues long after the placement of the device on the market. The predicate notions of where regulation starts and ends do not apply as crisply as before. Effective medical device regulation must walk hand in hand with standards like IEC 80001 into the future, in much the same way as biomedical staff must now walk hand in hand with IT staff.

Good luck to everyone. Try a pilot implementation; you might like it.

Brian Fitzgerald
Deputy Division Director
Division of Electrical and Software Engineering
Center for Devices and Radiological Health
Office of Science and Engineering Laboratories
U.S. Food and Drug Administration

[1] See U.S. Food and Drug Administration. Structured Product Labeling Resources, available at www.fda.gov/ForIndustry/DataStandards/StructuredProductLabeling/default.htm.

CARE PROVIDER PERSPECTIVE

The impact of International Electrotechnical Commission (IEC) 80001-1 on our organization will not be as great as it is on other organizations. Information technology (IT) and clinical technology (CE) professionals already partner effectively on biomedical system rollouts. IT-network planning and design professionals understand that the network supports IT and biomedical systems. Our procurement processes include physician, nursing, IT, and clinical technology review of clinical workflow impact, IT standards fit, and clinical technology considerations. The benefit of IEC 80001-1 will be a formal increase in the visibility of biomedical devices and accelerated consolidation of IT and clinical technology backend management systems to provide an end-to-end view of IT and biomedical systems. The challenge will be melding IT and clinical technology culture to get the best of both worlds.

IEC 80001-1 represents a catalyst for a new level of IT and clinical technology cooperation to ensure network changes don't negatively impact biomedical systems. IEC 80001-1 is really about implementing processes, policies, and procedures to manage network change and biomedical system risk.

IT organizations already have change control, testing, and impact assessment in place for IT systems. Biomedical systems often fly under the IT radar and can be missed. IEC 80001-1 puts biomedical systems on the radar by creating the Medical IT-Risk Manager role. For organizations in which there is a close relationship between IT and clinical technology, IEC 80001-1 reinforces cooperation between them for network changes or additions of new biomedical devices. For organizations that don't have this close relationship between IT and clinical technology, IEC 80001-1 will help open up communication between the two.

The big change for clinical technology will be an increased requirement to use IT change management and configuration management systems for documentation, instead of the Risk Management File outlined in IEC 80001-1, which actually would move system management backwards. There also will be increased pressure to consolidate other clinical technology systems, such as asset management systems. The challenge will be leveraging IT systems for the tried-and-true ability to manage tens of thousands of complex IT systems while ensuring that clinical technology requirements are met.

The enhanced levels of vendor documentation regarding configurations, known issues, and hazards will help IT vendors understand biomedical systems requirements and what is important. However, enhanced documentation does not diminish the need for vendors to be active partners in risk management by embracing standards to help reduce risk. IT and clinical technology will need to work with organizations such as Medical Device "Plug-and-Play" Interoperability Program (MD PnP™) and implement contractual requirements such as Medical Device "Free Interoperability Requirements for the Enterprise" (MD FIRE) to ensure vendors participate in creating an environment that reduces variation and facilitates managing risk.

IEC 80001-1 is a positive step in acknowledging that modern biomedical systems are part of the IT environment—and that IT and clinical technology partnerships are critical in providing modern healthcare.

Major U.S. Healthcare System

MEDICAL DEVICE MANUFACTURER PERSPECTIVE

The risk management process has become a cornerstone of a structured approach for medical device manufacturers to meet product health and safety requirements. A risk-based approach for dealing with health and safety requirements is not new. Manufacturers of medical devices have been using elements of a risk management process for decades. However, what was missing was a systematic, fact-based, life cycle-oriented method for applying the principles of risk management to the design, manufacture, deployment, and decommission of medical devices. The ISO 14971 process is a life cycle approach that begins at the earliest stages of product design and continues through the manufacture and deployment of the medical device, ending with its ultimate decommissioning. Since its publication in 2000, ISO 14971 has become the globally recognized standard used by manufacturers of all sizes and types in implementing and operating a risk management system for medical devices.

When applying ISO 14971, a manufacturer soon realizes there are limits to what it can do to manage the ultimate risks associated with the use of its medical device. The medical device user must be a partner in the process. Nowhere is that more evident than with those medical devices that are intended to be integrated into a user-deployed and -managed IT-network. The manufacturer can provide tools to assist the user in managing foreseen risks. However, from the medical device manufacturer's point of view, the ad hoc nature of this environment means there can be risks for which it cannot provide effective risk control measures other than information for safety.

This is where IEC 80001-1 becomes an important element in the overall process of managing risk in the healthcare environment. It describes a process based on the principles of ISO 14971 and extends them to the integration of a medical device as part of a user-deployed and -managed IT-network. IEC 80001-1 provides a framework in which the stakeholders—those accountable for the use and maintenance of the IT-network, the providers of the IT equipment or software, and the medical device manufacturer—can collaborate effectively to manage risks that arise in a highly dynamic environment.

Subclause 3.5 of IEC 80001-1 details basic requirements for the information the medical device manufacturer needs to provide in the accompanying documents for devices intended to be connected to an IT-network. These requirements are consistent with those in product safety standards, such as IEC 60601-1, and thus place no extra burden on the medical device manufacturer.

However, IEC 80001-1 does describe how stakeholders can interact and how information can be communicated once the medical device is placed on the market. The standard describes the minimum requirements for a responsibility agreement between the stakeholders that includes the risk management activities covered, the information needed for the user to perform these activities, and the stakeholders' roles and responsibilities in managing potentially adverse events. It recognizes that, in some cases, those responsible for a particular implementation may need technical information that the medical device manufacturer believes is sensitive in nature and that special arrangements might be needed for the user to gain access to such information.

IEC 80001-1 provides a framework that sets up consistent expectations among the stakeholders. When implemented by a healthcare delivery organization, the standard helps medical device manufacturers understand what is expected of them and helps them prepare and deliver the required information in a systematic rather than an ad hoc way, leading to greater customer satisfaction and, ultimately, improved patient safety.

Charles Sidebottom, P.E.
Secretary, IEC Subcommittee 62A, Common aspects of electrical equipment used in medical practice

IT TECHNOLOGY INDUSTRY PERSPECTIVE

Health IT systems and electronic medical devices are increasingly being called upon to share network resources and in some cases to interoperate. This introduces potential for new hazardous situations to arise, such as:

- Unintended operation of medical devices
- Mutual interference between medical devices and other systems attached to the network
- Unmanaged contention for resources on the network
- Delays in information flow between health IT systems and medical devices
- Issues with semantics/accuracy, timing, or format of the data communicated
- Confusion about the medical records to which patient data from medical device belongs

As a systems integrator, British Telecom Health already undertakes clinical safety and security management activities for the networked services that we deliver to health providers, in accordance with our own quality management systems. Our customers already undertake some assurance activities as part of the acceptance into service of those services.

The introduction of IEC 80001 provides health delivery organizations (HDOs) with a holistic framework for managing clinical and security-related risks throughout the life of a network. With more technology integrating with medical devices, the increasing risks to patient safety require further attention. In successfully implementing IEC 80001, HDOs will have an additional toolset to promote their ability to deliver safe and effective healthcare.

Martin Ellis
Director, Patient Safety
British Telecom Health

INTRODUCTION

IS THERE A PROBLEM?

During the first meeting of the team that developed the International Electrotechnical Commission (IEC) 80001-1 standard, the question was asked: “Is there really a problem here? Or are we attempting to create a solution looking for a problem or take an approach that could be addressed using existing standards and technologies?” From that first January 2007 meeting in San Diego, CA, the immediate response was, “Oh, yes, there is a problem!” Moreover, it has become increasingly evident that 80001 is the right standard at the right time. The underlying causes for its creation have increased significantly, to the point where some are calling it “the most anticipated medical device standard in recent memory!” Why?

Part of the problem results from the ever-increasing reliance on health information technology (HIT) to support and enhance healthcare delivery around the world. The risks inherent in treating patients are very well understood by healthcare delivery organizations (HDOs) and clinicians, but extending consideration of causes of risks to the network infrastructure that provides tools to support care is often overlooked. The primary benefits of HIT are well documented: namely, improved patient safety, quality of care, and clinical workflow efficiency. However, realizing these benefits is a different matter. Anyone who has been paying even casual attention can cite anecdotes from personal experience or from recent front pages of their local newspapers. For example:

- Wireless infusion pumps are deployed throughout a hospital and well integrated into clinical workflow, but the entire wireless network goes down for more than a day when drug library updates are pushed out to the devices, resulting in “secondary” alarm communication failure and delayed clinical response.[2]
- Who would have guessed that installing Microsoft Office to read documentation on the same server being used to monitor home health patients could result in a deadlock that took down not only the PBX but an entire public phone exchange![3]
- Why did that system reboot right in the middle of surgery? Perhaps applying a security patch to a system in the operating room should have been better coordinated to ensure that medical systems being actively used were not updated until there was no risk to any patient. By subsequently stopping all applications of the security patch, though, the entire hospital was infected with the Conflicker worm, going from bad to worse![4]

[2] Although this is a true anecdote, published patient safety incidents that are directly tied to failure of network technology are hard to come by. As stated in The Joint Commission’s Sentinel Event Alert #42 (2008 December), “There is a dearth of data on the incidence of adverse events directly caused by HIT overall.” See also footnote 5 and Schrenker R. Networking—failures and consequences. 24x7. 2009 (July). This remains a significant challenge.

[3] See **Clarke M, and Jones R**. Newham home monitoring for long term conditions. Technical report. Brunel University, West London.

[4] There are many examples of this issue across the globe, including **Williams C**. Conflicker seizes city’s hospital network. *The Register*. 2009 (January 20). Available at www.theregister.co.uk/2009/01/20/sheffield_conficker/.